base for terrorists who want to kill as many of our people as they possibly can.''

These are clear words, Madam Speaker. Those words, if they were U.S. policy, would give solace to our allies, to the Afghans, to the Pakistanis and to our own troops taking the fight to the Taliban. But our actual intentions in Afghanistan are not clear, even though General McChrystal's report states explicitly that without more troops in the next year, the United States faces mission failure where defeating the insurgents is no longer possible. That's the view of a respected general, the commander handpicked by President Obama, who works in Kabul and travels around Afghanistan every day.

So why is it that the Obama administration is sending mixed signals to the American public and to the rest of the world? Why is his national security adviser on Sunday morning talk shows saying that Afghanistan is not in imminent danger of falling to the Taliban? After many years of fighting in Afghanistan, after many years of two steps forward and one step back, we cannot flinch. We must let our allies, our military and the Afghans and Pakistanis know right now that we will do what it takes to provide stability and security.

Governing is about tough decisions. We must make the tough decisions to give General McChrystal the troops he needs to finish this mission. We must protect the population and assure them that we're not going anywhere. That's our only hope of winning over the Afghan people who fear that if they work with us, they'll be slaughtered by the Taliban when the Americans leave. As President Obama said just 2 months ago: ''This will not be quick nor easy. But we must never forget: This is not a war of choice. This is a war of necessity.''

Let's hope that he has not forgotten.

CYBERSECURITY

The SPEAKER pro tempore. Under a previous order of the House, the gentleman from Texas (Mr. BURGESS) is recognized for 5 minutes.

Mr. BURGESS. I thank the Speaker for the recognition.

I come to the floor tonight to talk about cybersecurity. We all hear about data breaches. They're so common, it seems like you can hardly pick up the newspaper without reading about another occurrence. And unfortunately, the rate at which they're occurring is also increasing. A report in 2009 found that more electronic records were breached in 2008 than in the previous 4 years combined. Almost 10 million United States adults were victims of identity theft in 2008. These are expensive. A 2009 report found that the average cost of a data breach had risen to $202 per customer from last year's $197. Over $600 is lost out of pocket per second to identity fraud, costing consumers and businesses over $52 million a day.

Examining some of the sources of the breaches, 29 percent come from government and military, 28 percent are from educational institutions, 22 percent in general business, 13 percent in health care companies, 8 percent in banking, credit card and financial services. Within the government itself, on the May 2008 Federal Security Report Card, the Department of Interior, the Department of Treasury, the Department of Veterans Affairs and the Department of Agriculture all scored failing grades.

Within the military, the personnel data of tens of thousands of United States soldiers has been downloaded by unauthorized computer users. The data included Social Security numbers, blood type, cell phone numbers, e-mail addresses and the names of soldiers' spouses and children. A 2006 Department of Veterans Affairs data breach put almost 30 million veterans' names, addresses and Social Security numbers at risk.

Within the retail segment, in 2009, a Miami man was charged in the largest case of computer crime and identity theft ever prosecuted. He, along with two unknown Russian coconspirators, were charged with taking more than 130 million credit card and debit card numbers from late 2006 to early 2008, and they did it as an inside job. They reviewed lists of Fortune 500 companies, decided where to aim; they visited the stores to monitor the payment systems used; they placed sniffer programs on corporate networks; and the programs intercepted credit card transactions in real time and transmitted the numbers to computers in the United States, Netherlands and the Ukraine. An expert said the case provided more evidence that retailers and banks needed to strengthen, needed to harden, industry standards.

And finally, educational institutions. As I noted earlier, second only to government and data breaches are educational institutions, probably the most disturbing statistic. In 2007, the number of data security breaches in colleges and universities increased almost two-thirds from 2006, and the number of educational institutions affected increased by almost three-quarters. In August of 2005, hackers stole almost 400,000 electronic records of current, former and prospective students in my congressional district at the University of North Texas. The hackers got away with names, addresses, telephone numbers, Social Security account numbers and possibly credit card numbers.

So what can we do? Of the breaches, 87 percent are considered avoidable if reasonable controls had been in place. Madam Speaker, now is the time for Congress to enact a meaningful national standard to protect commercial and government data. This requires leadership at the top levels of an organization to take an active role in ensuring that their systems are secure. Federal Government subcontractors that have access to sensitive and personally identifiable information should be required to comply with the same standards as Federal agencies and departments. Finally, we must all be involved from the top down and the bottom up. We must encourage leaders of government agencies and private enterprises to actively manage and rigorously protect the data collected and stored within their institutions. We must make this a priority, and Congress should take up and pass House Concurrent Resolution 193.

This bipartisan resolution, introduced by myself and CHARLIE GONZALEZ of Texas, expresses the Sense of Congress for the need to pass meaningful legislation to protect commercial and government data from data breaches. There are a lot of disturbing statistics. Let's take action now so that the occurrence, cost and individuals affected do not continue to increase.

CONGRESS MUST BE TRANSPARENT WITH VITAL LEGISLATION

The SPEAKER pro tempore. Under a previous order of the House, the gentlewoman from Michigan (Mrs. MILLER) is recognized for 5 minutes.

Mrs. MILLER of Michigan. Madam Speaker, our Nation currently has an unemployment rate of nearly 10 percent. In my home State of Michigan, it's actually over 15 percent. In the last fiscal year, our Federal budget deficit was over $1.4 trillion; and the Obama administration projects that over the next 10 years, our deficit will be over $9 trillion.

When dealing with our budget, difficult times like these require very decisive actions. Unfortunately, over the last year or so, as this Congress has racked up record-breaking deficits, we have seen legislation brought to the floor that forced massive new debt on the American people while giving Members little or no time to read any of the legislation.

Last fall, the Bush administration and the leadership of this House asked the House to vote on a $700 billion bailout for Wall Street with no strings attached on how the money would be spent. I was proud to vote ''no'' on that Wall Street bailout. Unfortunately, that bill did pass this House, and it became law. The result has been a program that has been widely rejected by the American people.

Then in February, President Obama asked Congress to pass an economic stimulus plan, and many on our side of the aisle were ready to help. In fact, we proposed a bill that, according to a formula used by President Obama's own economic advisers, would produce twice the jobs at half the cost. Instead, the Democrats crafted a bill behind closed doors. They filed a 1,073-page conference report in the middle of the night and asked Members of this House to vote on $787 billion of deficit spending while not one single Member of this